Současné teroristické hrozby a připravenost ČR na ně reagovat

Bc. Eliška Rovenská MBA

Předmět: Bezpečnostní management a působnost orgánů ČR

29.4.2025

Jaké jsou současné teroristické hrozby

Současné teroristické hrozby zahrnují obecně několik klíčových oblastí relevantní i pro ČR:

- **Islámský radikalismus**: Tento typ terorismu je v Evropě nejčastěji spojován s radikálními islamistickými skupinami, jako je Islámský stát, Al-Káida nebo Boko Haram v Africe.
- **Politický extremismus**: Pravicový i levicový extremismus v Evropě v současné době sílí. V ČR jsou oba směry dlouhodobě monitorovány, a přestože riziko teroristických útoků těchto skupin není vysoké, jsou jejich aktivity průběžně sledovány.
- **Osamělí útočníci**: I samostatně jednající jednotlivci mohou představovat významnou hrozbu. Příkladem je střelba na Filozofické fakultě UK v Praze v r. 2023 nebo v restauraci Družba v Uherském Brodě v r. 2015 (i když z hlediska motivace je nelze zcela považovat za teroristické útoky, protože motivem byly osobní a ne zcela objasněné cíle).
- **Kybernetické hrozby**: Teroristické skupiny stále častěji využívají kybernetické útoky k dosažení svých cílů

Hlavní druhy současných teroristických hrozeb

Současné teroristické hrozby zahrnují různé formy násilí a útoků, které mají za cíl šířit strach a destabilizovat společnost. Mezi hlavní hrozby patří:

- **Kybernetický terorismus** – útoky na počítačové sítě a informační systémy.
- **Bombové útoky a výbušniny** – použití výbušnin k útokům na osoby, veřejná místa nebo budovy.
- **Únosy a držení rukojmích** – získání politických nebo finančních výhod.
- **Použití chemických, biologických nebo jaderných látek** – zvlášť nebezpečné útoky, mohou mít katastrofální důsledky.
- **Dezinformační kampaně** – šíření falešných zpráv (fake news), manipulace veřejného mínění.

V České republice je úroveň teroristických hrozeb relativně nízká, přesto je důležitá bdělost a rizika teroristických hrozeb nepodceňovat.

Formy současného terorismu

Současné teroristické hrozby zahrnují různé formy:

- **Domácí terorismus** zahrnuje jednotlivce nebo malé skupiny páchající teroristickou činnost na domácím území, tedy v ČR. Motivem může být např. prosazování politických, náboženských nebo ideologických cílů.
- **Mezinárodní terorismus** zahrnuje teroristické činy páchané v mezinárodním měřítku, např. organizacemi jako jsou Al-Káida nebo Islámský stát.
- **Kybernetický terorismus** využívá nové technologie, např. drony nebo umělou inteligenci. Působí v kyberprostoru jak na domácí, tak (častěji) i na mezinárodní úrovni.

Islámský radikalismus a politický extremismus

S teroristickou hrozbou v současné Evropě je nejčastěji spojován islámský radikalismus.

- Osoby hlásící se k radikálně islamistické ideologii, případně přímo napojené na mezinárodní teroristické organizace spáchaly v Evropě řadu útoků, které si v poslední době získaly větší pozornost veřejnosti.
- K Islámskému státu se přihlásili např. teroristé, kteří spáchali střelecký útok v koncertní síni Bataclan v Paříži v roce 2015 nebo aktéři sebevražedných explozí na letišti Zaventem a v bruselském metru v roce 2016.
- České republice je úroveň nebezpečí teroristického útoku ze strany islámských radikálů nebo politických extremistů relativně nízká, ale je důležité tyto potenciální hrozby nepodceňovat.

Kybernetický terorismus

Kybernetický terorismus je forma terorismu, která využívá anonymity kyberprostoru k útokům na počítačové sítě, informační systémy a data. Mohou narušit klíčovou infrastrukturu státu.

Cílem těchto útoků je způsobit chaos, narušit infrastrukturu nebo zastrašit vlády i veřejnost.

Mezi hlavní charakteristiky kybernetického terorismu patří:

- **Politická motivace** – útoky jsou často zaměřeny na dosažení politických nebo ideologických cílů.
- **Použití technologií** – sociální inženýrství a umělá inteligence, které využívají ke zdokonalení phishingových kampaní nebo ransomwarových útoků.
- **Dopad na reálný svět** – i když se útoky odehrávají ve virtuálním prostoru, jejich důsledky mohou být velmi reálné, například narušení dodávek energie, firemních nebo bankovních systémů, zdravotnických služeb, odcizení nebo zašifrování dat apod

Aktuální trendy kybernetického terorismu

- **Útoky na kritickou infrastrukturu** – zasaženy mohou být zdravotnické systémy, energetické sítě a další pro stát klíčové sektory.
- **Zneužití internetu věcí (IoT)** – s rostoucím počtem připojených zařízení se zvyšuje riziko útoků na průmyslová zařízení, dopravní systémy, chytrá města nebo i domácnosti.
- **Kryptoměnové podvody** – prostředky v kryptoměnách získané např. pomocí sociálního inženýrství, které jsou anonymní a těžko dohledatelné, útočníci využívají k financování svých aktivit.
- **Šíření malwaru** – špionážní a vyděračské malware
- **Útoky typu DDoS** (Distributed Denial of Service) – vyřazení důležitých webů z provozu, např. webů státní správy, k těmto napadením je časté využití botů.
- **Krádeže dat** a jejich následné zneužití

Tyto útoky mohou mít vážné důsledky pro ekonomiku, bezpečnost nebo i důvěru veřejnosti.

Prevence kybernetických hrozeb

- **Zvyšování povědomí o těchto hrozbách** – vzdělávání veřejnosti i organizací a firem, seznamování se s riziky, šíření informací o bezpečnostních opatřeních.
- **Nulová důvěra (Zero Trust přístup)** – model „nevěř, vždy ověřuj“, je to souhrnná strategie, která minimalizuje riziko neoprávněného přístupu.
- **Kybernetická odolnost** – organizace a firmy by měly mít plány reakce na incidenty a vypracovaná pravidla pro bezpečné zálohování dat.
- **Mezinárodní spolupráce** – sdílení informací mezi státy a organizacemi pomáhá lépe čelit globálním kybernetickým hrozbám.

Dezinformační kampaně

- **Šíření falešných zpráv za účelem manipulace veřejného mínění v ČR v současnosti stále sílí a boj státních orgánů proti dezinformacím přes veškeré proklamace stále není příliš efektivní.**
- Nedávno proběhlé komunální volby, povodně na Moravě nebo nadcházející parlamentní volby přitahují velké množství falešných zpráv (fake news).
- Na známých dezinformačních webech, které se tváří jako zpravodajské, ale neřídí se základními novinářskými principy, se objevuje množství manipulativních článků, upravených fotografií nebo deepfake videí.
- **Dezinformační scéna se stále více radikalizuje.** Je to zřejmé nejen na dezinformačních webech, ale také na sociálních sítích.
- Nejen v ČR, ale prakticky v celé Evropě se v poslední době se **prosazují uskupení s radikálními názory hraničícími až s fašismem.** Ke svému prosazování využívají **populistickou rétoriku**.

Připravenost ČR reagovat na teroristické hrozby

- **Zpravodajské a bezpečnostní složky** – BIS, ÚZSI, Vojenské zpravodajství
- **Právní rámec** - terorismus je v České republice trestným činem dle trestního zákoníku (zákon č. 40/2009 Sb.).
- **Preventivní opatření** - Pravidelné proticvičení teroristických útoků a krizová školení pro policii, armádu a záchranné složky,
- **Bezpečnostní audity kritické infrastruktury**
- **Protiteroristická agenda EU a Programu obrany proti terorismu NATO**
- **Ministerstvo vnitra ČR** – Odbor bezpečnostní politiky
- **Centrum proti terorismu a hybridním hrozbám (CTHH)** - speciální útvar MV

Bezpečnostní a zpravodajské složky ČR v boji proti terorismu

- **BIS (Bezpečnostní informační služba)** – BIS se zaměřuje na prevenci mezinárodního terorismu, zejména islámského radikalismu, a sleduje aktivity jako propagandu, nábor a financování teroristických sítí, přičemž klíčovým signálem je radikalizace. Prostřednictvím mezinárodní spolupráce odhaluje hrozby na území ČR, přičemž aktuálním trendem jsou útoky osamělých útočníků na měkké cíle pomocí improvizovaných prostředků.
- **ÚZSI (Úřad pro zahraniční styky a informace)** – civilní rozvědka. Získává informace v zahraničí, které se mohou týkat bezpečnosti ČR. Zaměřuje se na mezinárodní teroristické sítě a jejich plány.
- **Vojenské zpravodajství** – pracuje pro armádu. Získává, shromažďuje a vyhodnocuje informace, které svědčí o riziku terorismu, organizovaného zločinu a sabotáží. Spolupracuje se zahraničními armádami a NATO.
- **Policie ČR** – Na boj proti terorismu a organizovanému zločinu se v rámci Policie ČR zaměřují tři specializované celostátní útvary: Národní centrála proti terorismu, extremismu a kybernetické kriminalitě, Národní centrála proti organizovanému zločinu a Národní protidrogová centrála.

Právní rámec a preventivní opatření proti terorismu v ČR

Právní rámec

- **Trestní zákoník (zákon č. 40/2009 Sb.)** – definuje terorismus jako trestný čin. Zahrnuje plánování, financování, přípravu a spáchání teroristického činu, a také jeho podporu.

Preventivní opatření

- **Proticvičení a krizová školení** – pravidelné simulace teroristických útoků (např. v metru, školách nebo letištích), kde si policie, armáda a IZS trénují rychlou reakci, komunikaci a záchranné postupy.
- **Bezpečnostní audity kritické infrastruktury** – Kritická infrastruktura zahrnuje klíčové prvky, jejichž narušení by mohlo vážně ohrozit bezpečnost státu, a její ochrana je součástí protiteroristické strategie ČR. Stát ve spolupráci s provozovateli (veřejnými i soukromými) zavádí bezpečnostní standardy, krizové plány a komunikační mechanismy, aby minimalizoval rizika útoků na tyto cíle, včetně teroristických.

Preventivní opatření proti terorismu v ČR

Protiteroristická agenda EU a NATO

- **EU** – Dokument Protiteroristická agenda pro EU: předvídání, prevence, ochrana a reakce. Zaměřuje se na předvídání hrozeb, prevenci radikalizace, ochranu veřejných prostor a efektivní reakci na teroristické útoky. Cílem je vytvořit koordinovaný a flexibilní rámec pro boj proti terorismu, který chrání evropské hodnoty a bezpečnost občanů.
- **NATO** – vnímá terorismus jako jednu z hlavních hrozeb. ČR spolupracuje na cvičeních, sdílení informací a plnění **Programu obrany proti terorismu**, který se zaměřuje na ochranu sil, kyberbezpečnost a boj proti CBRN hrozbám (chemickým, biologickým, radiačním, jaderným).

Ministerstvo vnitra ČR – Odbor bezpečnostní politiky

- aktivně se podílí na prevenci a potírání terorismu, zaměřuje se na prevenci radikalizace, ochranu kritické infrastruktury a rozvoj schopností pro včasné odhalování hrozeb. Spolupracuje s mezinárodními organizacemi, jako jsou NATO, EU a OSN, a podílí se na formulování protiteroristických strategií, včetně boje proti financování terorismu a posilování bezpečnostních kapacit.

Centrum proti terorismu a hybridním hrozbám (CTHH)

- zaměřuje se na monitorování a analýzu hrozeb spojených s terorismem, včetně útoků na měkké cíle, extremismu a šíření dezinformací, které ohrožují vnitřní bezpečnost státu. Na základě této analýzy centrum navrhuje a implementuje řešení, včetně legislativních opatření, a šíří odborné informace o těchto problémech mezi veřejnost a odborníky.

Závěr

V současnosti jsou v ČR nejnebezpečnější kybernetické útoky a zmíněné dezinformační kampaně.

Obě tyto hrozby vykazují rychlý vzestup a jsou stále agresivnější a sofistikovanější.

Na závěr bych ráda ještě zmínila, že v ČR působí **internetová skupina Čeští elfové, která si klade za cíl boj s dezinformačními kampaněmi a ruskou propagandou v českém kyberprostoru.** Více informací na https://cesti-elfove.cz/

Skupina se zformovala v roce 2018 po vzoru obdobných skupin v pobaltských státech. Mluvčím Českých elfů je Vít Kučík.

Děkuji za pozornost a dotazy

Bc. Eliška Rovenská MBA

eliska.rovenska@cevro.cz

Odkaz na zdroj obrázku

Grohmann, Jan. Teroristické útoky v roce 2013. Armádní noviny [online]. 12. února 2014 [cit. 26. dubna 2025]. Dostupné z: https://www.armadninoviny.cz/statistika-teroristicke-utoky-v-roce-2013.html

Odkazy na zdroje

- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor bezpečnostní politiky. *Bezpečnostní hrozby* [online]. 17. června 2019 [cit. 26. dubna 2025]. Dostupné z: https://mv.gov.cz/clanek/bezpecnostni-hrozby-337414.aspx
- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Centrum proti hybridním hrozbám. *Typologie terorismu* [online]. 17. června 2019 [cit. 26. dubna 2025]. Dostupné z: https://mv.gov.cz/chh/clanek/terorismus-a-mekke-cile-typologie-terorismu-typologie-terorismu.aspx
- SYSTEM4U. *Aktuální trendy v oblasti kybernetické bezpečnosti* [online]. 30. září 2024 [cit. 26. dubna 2025]. Dostupné z: https://www.system4u.cz/blog/aktualni-trendy-v-oblasti-kyberneticke-bezpecnosti/
- ISVS. *DVS: 7 klíčových kybernetických hrozeb + trendy pro rok 2025* [online]. 2024 [cit. 26. dubna 2025]. Dostupné z: https://www.isvs.cz/dvs-7-klicovych-kybernetickych-hrozeb-trendy-pro-rok-2025/
- LEGISLATIVA.CZ. *Kybernetický útok* [online]. 2024 [cit. 26. dubna 2025]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Typologie terorismu* [online]. 2024 [cit. 26. dubna 2025]. Dostupné z: https://mv.gov.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09Mg%3D%3D

Odkazy na zdroje

- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Typologie terorismu* [online]. 2024 [cit. 26. dubna 2025]. Dostupné z: https://mv.gov.cz/chh/clanek/terorismus-a-mekke-cile-typologie-terorismu-typologie-terorismu.aspx
- CLARKE, Colin P. *Trends in Terrorism: What's on the Horizon in 2025?* [online]. 2025 [cit. 26. dubna 2025]. Dostupné z: https://www.fpri.org/article/2025/01/trends-in-terrorism-whats-on-the-horizon-in-2025/
- GLOBAL FIGHT AGAINST TERRORISM FOUNDATION. *An Insight into Global Terrorism Trends 2024* [online]. 2024 [cit. 26. dubna 2025]. Dostupné z: https://www.gfatf.org/archives/an-insight-into-global-terrorism-trends-2024/
- BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. *Terorismus* [online]. [cit. 26. dubna 2025]. Dostupné z: https://www.bis.cz/terorismus/
- ÚŘAD PRO ZAHRANIČNÍ STYKY A INFORMACE. *Jaké je vaše hlavní poslání?* [online]. [cit. 26. dubna 2025]. Dostupné z: https://www.uzsi.cz/jake-je-vase-hlavni-poslani
- ÚŘAD PRO ZAHRANIČNÍ STYKY A INFORMACE. *Kdo jsme* [online]. [cit. 26. dubna 2025]. Dostupné z: https://www.uzsi.cz/kdo-jsme
- VOJENSKÉ ZPRAVODAJSTVÍ. *Kdo jsme* [online]. [cit. 26. dubna 2025]. Dostupné z: https://vzcr.gov.cz/kdo-jsme-35

Odkazy na zdroje

- POLICIE ČESKÉ REPUBLIKY. *Zveřejněné informace 2024: Terorismus a organizovaný zločin* [online]. [cit. 26. dubna 2025]. Dostupné z: https://policie.gov.cz/clanek/zverejnene-informace-2024-terorismus-a-organizovany-zlocin.aspx
- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Ochrana kritické infrastruktury* [online]. [cit. 26. dubna 2025]. Dostupné z: https://mv.gov.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx
- EVROPSKÁ KOMISE. *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond* [online]. 9. prosince 2020 [cit. 26. dubna 2025]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020DC0795
- MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. *Boj proti terorismu* [online]. [cit. 26. dubna 2025]. Dostupné z: https://mzv.gov.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/boj_proti_terorismu/index.html
- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Analýza rizik* [online]. [cit. 26. dubna 2025]. Dostupné z: https://mv.gov.cz/docDetail.aspx?docid=22028750&docType=ART